

Na podlagi tretjega odstavka 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18) minister za javno upravo izdaja

PRAVILNIK **o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave**

I. SPLOŠNE DOLOČBE

1. člen **(vsebina)**

Ta pravilnik podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov in minimalni obseg ter vsebino varnostnih ukrepov organov državne uprave.

2. člen **(pomen izrazov)**

Izrazi, uporabljeni v tem pravilniku, pomenijo:

1. Celovitost je lastnost informacij, omrežij in informacijskih sistemov, da so točni in popolni.
2. Ključni, krmilni in nadzorni informacijski sistemi in deli omrežja ter pripadajoči podatki so informacijski sistemi in deli omrežja ter pripadajoči podatki organov državne uprave (v nadaljnjem besedilu: ODU), ki so bistvenega pomena za delovanje storitev ODU.
3. Neprekinjeno poslovanje so aktivnosti, ki so potrebne za ohranjanje poslovanja organizacije v času motenj ali prekinitev normalnega delovanja.
4. Razpoložljivost je lastnost informacij, omrežij in informacijskih sistemov, da so dostopni in uporabni na pooblaščno zahtevo.
5. Sistem upravljanja neprekinjenega poslovanja je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se na njih odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni ter vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov (v nadaljnjem besedilu: SUNP).
6. Sistem upravljanja varovanja informacij je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov (v nadaljnjem besedilu: SUVI).
7. Sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za ODU in ki zato zahteva zaščito.
8. Trajanje incidenta je časovno obdobje od prekinitve ustreznega zagotavljanja storitve v smislu razpoložljivosti, celovitosti ali zaupnosti do trenutka njene ponovne vzpostavitve.
9. Uporabnik je fizična ali pravna oseba, ki uporablja posamezno storitev ODU neposredno, posredno ali s posredovanjem oziroma je odvisna od nje.
10. Zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom.

II. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

3. člen **(vsebina in struktura varnostne dokumentacije)**

(1) ODU vzpostavijo in vzdržujejo dokumentiran SUVI in SUNP, ki mora obsegati najmanj elemente iz prvega odstavka 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18).

(2) Varnostno dokumentacijo iz prejšnjega odstavka tega člena podpiše predstojnik ODU.

(3) Če ima ODU za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni v skladu s tem pravilnikom.

4. člen **(analiza obvladovanja tveganj)**

Analiza obvladovanja tveganj z oceno sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza obvladovanja tveganj) obsega najmanj:

1. navedbo sredstev znotraj SUVI in upravljavce teh sredstev,
2. navedbo potencialnih groženj tem sredstvom,
3. navedbo ranljivosti sredstev iz 1. točke tega člena, ki bi jih lahko grožnje iz prejšnje točke prizadele,
4. navedbo vpliva uresničitve groženj iz 2. točke tega člena na razpoložljivost, celovitost in zaupnosti sredstev iz prve točke tega člena zaradi ranljivosti iz prejšnje točke,
5. oceno vpliva na opravljanje storitev ODU v primeru kršitve informacijske varnosti zaradi izgube razpoložljivosti, celovitosti ali zaupnosti,
6. realistično oceno verjetnosti, da pride do kršitve informacijske varnosti,
7. ovrednotenje ravni tveganj in
8. določitev sprejemljive ravni tveganj.

5. člen **(politika neprekinjenega poslovanja)**

Politika neprekinjenega poslovanja z načrtom njegovega upravljanja (v nadaljnjem besedilu: politika neprekinjenega poslovanja) obsega najmanj:

1. navedbo postopkov neprekinjenega poslovanja, ki se jo izdela na podlagi popisa poslovnih procesov,
2. oceno vpliva na poslovanje, ki zajema navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije znotraj ODU in odpovedi storitev pogodbenih izvajalcev,
3. določitev minimalne ravni poslovanja,
4. navedbo ukrepov za zagotavljanje neprekinjenega poslovanja, ki se izdela na podlagi ocene vpliva na poslovanje iz 2. točke tega člena in minimalne ravni poslovanja iz prejšnje točke ter
5. določitev vlog in odgovornosti za izvajanje politike neprekinjenega poslovanja in njeno posodabljanje.

6. člen **(seznam ključnih sistemov)**

Seznam informacijskih sistemov in delov omrežja ODU ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev ODU, obsega najmanj:

- navedbo sredstev znotraj SUVI, od katerih je odvisno zagotavljanje storitev ODU, in
- seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov (v nadaljnjem besedilu: ključni sistemi) in navedbo njihovih upravljavcev.

7. člen **(načrt obnovitve delovanja ključnih sistemov)**

Načrt obnovitve in ponovne vzpostavitve delovanja ključnih sistemov iz prejšnjega člena (v nadaljnjem besedilu: načrt obnovitve delovanja ključnih sistemov) zajema opis odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

8. člen **(načrt odzivanja na incidente)**

(1) Načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave (v nadaljnjem besedilu: načrt odzivanja na incidente) obsega najmanj:

1. opis sistema za zaznavo incidentov informacijske varnosti,
2. opis sistema za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo,
3. opis postopkov za odziv, obravnavo in analizo incidentov informacijske varnosti, vključno z beleženjem vseh odzivnih aktivnosti,
4. opis odgovornosti oseb oziroma organizacijskih enot, ki jih je treba vključiti v aktivnosti iz prejšnje točke,
5. opis postopkov in odgovornosti za poročanje o incidentih znotraj ODU in izven ODU ter
6. opis protokola obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave.

(2) Obvestilo iz 6. točke prejšnjega odstavka se pošlje CSIRT organov državne uprave na način, kot je objavljen na njegovi spletni strani in zajema najmanj:

1. oceno števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvenih storitev,
2. oceno trajanja incidenta,
3. oceno geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
4. oceno morebitnega medresorskega vpliva incidenta in
5. oceno pomembnosti vpliva incidenta na neprekinjeno izvajanje storitev ODU (lažji incident, težji incident, kritični incident).

(3) Opis protokola obveščanja iz 6. točke prvega odstavka tega člena se lahko smiselno uporabi za obveščanje pristojnega nacionalnega organa za informacijsko varnost, če ima ODU lastne zmogljivosti vsaj na ravni varnostno operativnega centra.

9. člen **(načrt varnostnih ukrepov)**

(1) Pri izdelavi načrta varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov ODU upoštevajo:

- dokumente varnostne dokumentacije iz 3. do 8. člena tega pravilnika in
- posebne potrebe delovnega področja ODU.

(2) Načrt varnostnih ukrepov iz prejšnjega odstavka vsebuje navedbo ukrepov, ki so:

1. učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje,
2. prilagojeni tako, da se prizadevanja ODU usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost in se izogibajo podvajanjem,
3. skladni tako, da se primarno obravnavajo osnovne in skupne varnostne ranljivosti ODU, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna delovna področja,
4. sorazmerni s tveganji tako, da se izogiba prekomernemu bremenu za ODU,
5. konkretni tako, da ODU te varnostne ukrepe izvajajo in da ti ukrepi prispevajo h krepitvi njihove informacijske varnosti,
6. preverljivi tako, da lahko na zahtevo pristojnega organa predložijo dokazila o njihovi implementaciji,
7. vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sistemov.

III. METODOLOGIJI ZA PRIPRAVO ANALIZE OBVLADOVANJA TVEGANJ IN ZA DOLOČITEV KLJUČNIH SISTEMOV

10. člen

(metodologiji za pripravo analize obvladovanja tveganj in za določitev ključnih sistemov)

(1) ODU analizo obvladovanja tveganj pripravi tako, da:

1. izvede popis sredstev znotraj SUVI in določi njihove upravljavce,
2. prepozna možne grožnje za izgubo celovitosti, razpoložljivosti in zaupnosti sredstev iz prejšnje točke,
3. prepozna ranljivosti sredstev iz 1. točke tega odstavka, ki bi jih lahko grožnje iz prejšnje točke prizadele,
4. oceni stopnjo vpliva uresničitve groženj iz 2. točke tega odstavka na razpoložljivost, celovitost in zaupnost sredstev iz 1. točke tega odstavka zaradi ranljivosti iz prejšnje točke,
5. oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi,
6. ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev ter
7. določi oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj.

(2) ODU seznam svojih ključnih sistemov pripravi tako, da:

- izmed popisanih sredstev znotraj SUVI iz 1. točke prejšnjega odstavka presodi, ali je zagotavljanje storitev ODU odvisno od posameznega sredstva znotraj SUVI, in
- izmed posameznih sredstev znotraj SUVI, od katerih je v skladu s prejšnjo alinejo odvisno zagotavljanje storitev ODU, presodi, katero izmed teh sredstev je bistveno za delovanje storitve ODU.

(3) ODU izvede analizo obvladovanja tveganj in določi ključne sisteme tako, da bodo rezultati teh postopkov dosledni, primerljivi in verodostojni.

ODU izvaja analizo obvladovanja tveganj ter določa ključne sisteme v rednih časovnih presledkih ali kadar so predlagane ali nastanejo bistvene spremembe v okviru SUVI.

IV. MINIMALNI OBSEG IN VSEBINA VARNOSTNIH UKREPOV

11. člen
(minimalni obseg in vsebina varnostnih ukrepov)

ODU za zagotavljanje celovitosti, zaupnosti, razpoložljivosti omrežij in informacijskih sistemov na podlagi varnostne dokumentacije iz 3. člena tega pravilnika pripravijo in izvajajo organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki zagotavljajo najmanj:

1. podporo predstojnika ODU zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni program dela ODU,
2. integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve,
3. notranjo presojo SUVI in SUNP v rednih časovnih presledkih,
4. upravljanje ključnih sistemov z določitvijo odgovornosti za njihovo zaščito,
5. ohranjanje dnevniških zapisov o delovanju ključnih sistemov iz prejšnje točke,
6. upravljanje prometa in komunikacij,
7. opredelitev varnostnih zahtev za ključne dobavitelje,
8. fizično in tehnično varovanje dostopov do prostorov, kjer so ključni sistemi,
9. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti ODU,
10. preverjanje identitete uporabnikov,
11. upravljanje pooblastil za dostop,
12. zagotavljanje ravni dostopnosti informacij,
13. zaščito pred zlonamerno programsko kodo,
14. beleženje dejavnosti ključnih sistemov, njihovih uporabnikov in administratorjev ter
15. zaznavanje poskusov vdorov in preprečevanje incidentov.

V. KONČNA DOLOČBA

12. člen
(začetek veljavnosti)

Ta pravilnik začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

Št. 386-3/2019/31
Ljubljana, dne 5. novembra 2019
EVA 2018-3130-0048

Rudi Medved
minister
za javno upravo